BİRLEŞMİŞ MİLLETLER TARAFINDAN GERÇEKLEŞTİRİLEN SİBER GÜVENLİK ÇALIŞMALARI

İbrahim AKDAĞ
Doktora Öğrencisi

Başlangıçta askeri bir proje olan bilgisayar ağları zamanla gelişme göstererek insan yaşamını etkisi altına almıştır. Bilgisayar ağları üzerinde gerçekleşen iletişim teknik bir kavramdan daha ileriye giderek içinde insan yaşamının başka bir boyutunu oluşturarak siber alanı yaratmıştır. Uluslararası bir kavram olan siber alan zamanla uluslararası pek çok konunun uygulama alanına dönüşmüş ve çeşitli güvenlik sorunları baş göstermeye başlamıştır. Günümüzde ülkeler kendi amaçlarını gerçekleştirme yolunda siber alandaki yeteneklerini kullanmaktan çekinmemekte zaman zamanda bu kabiliyetlerini karşı tarafa ciddi zararlar verecek şekilde kullanmaktadırlar (Puyvelde, 2019).

BM siber alana ilişkin ilk kararını 1998 yılında yayınlamıştır (A/RES/53/70 sayılı BM Kararı, 1998). 1996 yılında Güney Afrika'da gerçekleştirilmiş olan Bilgi Toplumu ve Gelişimi Konferansı ve yine aynı yıl Paris'te düzenlenmiş olan Terörizm konulu konferansta bilgi sistemleri güvenliğine ilişkin alınan kararlara dikkat çekilen bu karar metninde ülkelerin bu alandaki güvenlik tedbirlerini gözden geçirmeleri ve uluslararası çalışmalara katkı sağlamalarına ilişkin beklentiler belirtilmiştir. Siber alanın uluslararası suç işlenen bir ortam haline dönüşümü 80'li yıllarda başladığını göz önüne aldığımızda geç kalınmış bir karar olarak gözükmekle birlikte 90'lı yılların ortasından itibaren artan siber saldırılara BM'nin kayıtsız kalmadığı ortaya çıkmaktadır.

BM genel kurulu 1998 yılından itibaren her yıl konu ile ilgili bir karar yayınlamıştır. 2002 yılında yayınlanan karar gereği 2004 yılında konu ile ilgili çalışma yapmak için Ülke Uzmanları Grubu kurulmuştur (A/59/454 Sayılı BM Kararı, 2004). 1998 yılından 2000'li yılların ortalarına kadar ki yıllık kararlar-

da ülkelerin bu konuda dikkatli olmaları ön planda tutulurken, 2000'li yılların ortalarından itibaren bilgi teknolojilerindeki gelişimin kötü kullanılmasının insanlık için kötücül sonuçlarının olacağı vurgulanmaya başlanmış ve askeri alan dâhil pek çok alanda konu ile ilgili tedbirlerin alınması önerilmeye başlanmıştır. 2018 yılına kadar benzer bir içerik üzerinden ilerleyen kararlar 2018 yılında değiştirilmiş ve daha kapsamlı bir hal almıştır (A/RES/73/27 Sayılı BM Kararı, 2018). Ayrı başlıklar halinde ele alacağımız siber politikaların belirlenmesi, uzmanlar gurubu çalışmaları gibi konuların başlangıç adımları bu kararlar içinde yer almaktadır. Bu konu başlıklarına geçmeden önce 2018 yılı kararının içeriği detaylandırılacaktır.

Söz konusu kararda Bilgi teknolojilerinin ikincil kullanımı vurgulanarak kötücül amaçlarla kullanımının her zaman mümkün olduğu belirtilmektedir. Ülkelerin giderek artan miktarda askeri amaçları için bu teknolojilerden faydalanmaya başladığına dikkat çekilmektedir. Bilgi teknolojileri güvenliğinin sağlanmasında BM'nin liderlik etmesi gerektiği ve ülkeler arası diyalog kurulması konusunda daha çok çaba sarf edilmesi gerektiği tespiti yapılmaktadır. Üye ülkelerin iç hukuklarında konu ile ilgili düzenleme yapmaları ve hâkimiyet alanlarından üye devletlere karşı yapılan saldırıların engellemelerine yönelik tedbir almaları gerektiği belirtilmiştir. Bahse konu saldırıların hedef ülkenin egemenlik haklarına yönelik bir saldırı olduğu tanımlanması yapılmaktadır. Kararda konunun teknik yönüne ilişkin tespitlerde yer almaktadır. Örneğin siber saldırılarda sıkça kullanılan saldırı yazılımların alanda bilinen adıyla "tool"ların geliştirilmesi ve yayılmasına ilişkin tedbir alınması gerektiği vurgulanmaktadır. Hedef ülkelerin siber olay müdahale timlerinin çalışmalarını engellemeye yönelik saldırıların durdurulmasına yönelik tedbir alınması gerektiği belirtilirken SOME kavramı bir nevi sivil savunma alanı gibi değerlendirilmiş ve dokunulmazlığı vurgulanmıştır. Bu dokunulmazlığı silahlı çatışma hukukunda yer alan, harp alanındaki sağlık personelinin dokunulmazlığı ilkesine benzetmek mümkündür.

2010 yılından itibaren üye ülkeler BM kararlarında yer alan hususlara ilişkin raporlarını BM sekreterliğine sunmaktadır. Yıllık rapor adı altında yayınlanan ülke raporları ülkelerin konuya ilişkin bakış açılarını ve yaşanmakta olan gelişmelere karşı getirdikleri tepkileri içermektedir. Örneğin 2010 yılındaki ilk rapor belgesinde yer alan beş ülkeden bir tanesi olan Küba, ABD'yi Küba sınırları içerisinde yer alan elektromanyetik spektrumu işgal etmekle suçlamaktadır (A/RES/65/41 Sayılı BM Kararı, 2010). Yine aynı raporda Yunanistan bugün siber güvenliğin vazgeçilmez bir parçası olan risk değerlen-

dirmesi süreçlerinin küresel ölçekte tanımlanması gerektiği belirtmektedir. Müteakip yıllardaki raporlar incelendiğinde siber güvenlik konuları giderek ön plana çıkmaktadır. Ülkelerin Estonya ve Gürcistan örneklerinin tekrar yaşanmasını önlemek için uluslararası tedbirler alınması gerektiğine ilişkin önerileri sıkça yer almaktadır. Öte yandan raportör devletlerin ülkelerindeki alana yönelik hukuki düzenlemeleri ve kolluk kuvvetlerince konunun yakından takip edildiği ve özellikle siber suçlara ilişkin özel yapılar kurulduğu görülmektedir.

Türkiye 2013 ve 2019 yıllarında rapor sunmuştur (A/RES/68/243 Sayılı BM Kararı, 2013). 2013 ve 2019 yılı raporları karşılaştırıldığında ülkemizin 2013'te konmuş olan hedeflere hızla ulaştığını ve 2019 yılına kadar büyük bir değişim yaşadığı görülecektir. Türkiye 2019 raporunda, alana yaklaşımının geniş bir yelpazede olduğunu belirtmiş, siber güvenlikle ilgili ana sorumluluğun ulaştırma ve altyapı bakanlığında olmasına rağmen konunun daha kapsamlı olarak ele alındığı ve Aile, Çalışma ve Sosyal Hizmetler Bakanlığı, Milli Eğitim Bakanlığı dâhil pek çok kamu kurumu tarafından alana ilişkin faaliyetler gerçekleştirildiği somut örneklerle belirtilmiştir. Bu alanda gerçekleştirilen eğitimlerin önemi vurgulanmış ve gerçekleştirilmiş olan eğitim faaliyetleri, güvenli internet, USOM yapısı gibi projeler açıklanmıştır. Ülkede alanda yaşanan değişim örneklerle ortaya konmuş ve NATO ve AB gibi uluslararası organizasyonların düzenlemelere uyum sağlayarak üye olduğu uluslararası organizasyonlarda aktif olarak yer aldığı vurgulanmıştır.

BM Silahsızlanma Ofisi 2018 yılında yürürlüğe koyduğu Ortak Geleceğimizin Güvenliğini Sağlamak İçin Silahsızlanma Planı alana yönelik kapsamlı bir çalışmadır. Söz konusu çalışmanın 39 numaralı eylem maddesi "Siber Alanın Barışçıl Kullanımın Sağlanması ve Zararlı Aktivitelerin Önlenmesi" şeklindedir. 31. Maddesi ise "Siber alanın güvenliğinin sağlanması için ortaya çıkan normlara ilişkin üye ülkelerin söz konusu normlara olumlu katkı sunmasının sağlanması" olarak belirlenmiştir. Bahse konu eylem planı henüz başlangıç safhasında olduğu için siber alanla ilgili maddelerde kayda değer bir gelişme yaşanmamıştır. BM silahsızlanma ofisi Siber Politika portalını oluşturarak üye ülkelerin sunduğu güvenlik politikalarını bu portaldan sunmaktadır (Cyber Policy Portal, 2019). Üye ülkelerin resmi siber güvenlik dokümanları, siber güvenlik mimarisi, hukuki düzenlemeleri bu portal üzerinden erişilebilir durumdadır. Herhangi bir ülkenin siber alana ve güvenliğine ilişkin yaklaşımını bu dokümanlar üzerinden takip etmek mümkündür. AB, NATO, Şangay İş birliği Örgütü, Afrika Birliği, G7 gibi pek çok uluslararası örgütün konu ile ilgili resmi düzenlemeleri ve güvenlik mimarileri bu portal üzerinden erişilebilir durumdadır.

BM'nin alandaki çalışmaları incelendiğinde alana ilişkin genel bir tanımla yapıldığı, sorunların tespit edildiği, ülkeler arasında koordinasyon sağlandığı görülmekte ancak yaptırım gücü içeren net bir çalışma da bulunmamaktadır. BM'nin konuyu silahların kontrolü ve silahsızlanma alt başlığı altında ele aldığını belirtmiştik, üye ülkelerden gelen raporlar ve tepkilerde bu minvalde olmuş ve siber güç askeri güçle eşdeğer tutulmuştur. BM silahsızlanma konularında bu alanda olduğu gibi yaptırımdan uzak değildir. Kara Mayınlarının azaltılması, Nükleer Silahların Yayılımın Engellenmesi, Kimyasal ve Biyolojik silahların yasaklanması konularında BM ciddi başarılar elde etmiştir. Bu başarının temelinde ise insanlığın bu silahlardan ciddi zararlar görmesidir. Siber alanda yaşanan saldırılar ciddi bir artış içindedir, bu alanda yeterli bir uluslararası düzenleme bulunmamasından dolayı da yakın geleceğimizde insanlığı ciddi tehlikeler beklemektedir ve ilk kez karşılaşacağı pek çok tehditle yüz yüze gelebilecektir. Bilim kurgu vari bir öngörüde bulunacak olursak Siber alan şu an için insanların kontrolündedir ancak yapay zekanın kontrolsüz olarak siber alanla paralel olarak gelişimi bu alandaki kontrolün makinalara geçmesini olasılık dâhilindedir. Hepimizin bildiği "Terminatör" filmlerinde yer alan insanlığı hedef alan Skynet yapay zekâ programı en nihayetinde siber alanı hâkimiyet altına alarak başarıya ulaşmıştır, tüm o zeki makinalar iletişim için siber alanı kullanmaktadır. Bu ve benzeri kıyamet senaryolarına yaklaşıldıkça siber alanda güvenliği regüle eden uluslararası çalışmalar daha somut bir hal alacaktır. Bu çizgiye yaklaşıldığında BM şu an için etkisiz görülen çalışmaları ciddi bir altyapı oluşturacaktır. BM'nin sunduğu verilerde başka ülkelerde yaşanan gelişmeleri anlamak ve analiz etmek için önemli bir kaynakça oluşturmaktadır. Alanda yapılacak çalışmalarda bu verilerden yararlanmak çalışmalara başlangıçta iyi bir ivme kazandıracaktır.

Kaynakça

(2004). *A/59/454 Sayılı BM Kararı*. Birleşmiş milletler.

(1998). *A/RES/53/70 sayılı BM Kararı*. Birleşmiş Milletler.

(2010). *A/RES/65/41 Sayılı BM Kararı*. Birleşmiş Milletler.

(2013). *A/RES/68/243 Sayılı BM Kararı*. Birleşmiş Milletler.

(2018). *A/RES/73/27 Sayılı BM Kararı*. Birleşmiş Milletler.

Cyber Policy Portal. (2019). https://cyberpolicyportal.org/en/ adresinden alındı

Puyvelde, D. V. (2019). *Cybersecurity: Politics, Governance and Conflict in Cyberspace*. Wiley.